Description of document:	United States Army Intelligence and Security Command (INSCOM) Annual Command History, Fiscal Year 2001
Request date:	18-August-2007
Released date:	13-May-2014
Posted date:	30-June-2014
Source of document:	Freedom Of Information Act Request Commander, INSCOM ATTN: IAMG-C-FOI 4552 Pike Road Fort Meade, MD 20755-5995 Fax: (301) 677-2956

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

13 MAY 2014

This is in further response to your Freedom of Information Act (FOIA) request of August 18, 2007, for a copy of the INSCOM Annual History for FY2001 and supplements our letter of October 9, 2012.

Coordination has been completed with other elements of this command and other government agencies. The records have been returned to this office for our review and direct response to you.

We have completed a mandatory declassification review in accordance with Executive Order (EO) 13526. As a result of our review information has been sanitized and five pages are being withheld in their entirety as the information is currently and properly classified TOP SECRET, SECRET and CONFIDENTIAL according to Sections 1.2(a)(1), 1.2(a)(2), 1.2(a)(3) and 1.4(c) of EO 13526. This information is exempt from the public disclosure provisions of the PA as provided unter Title 5 U.S. Code 552 (k)(1) and of the FOIA pursuant to Title 5 U.S. Code 552 (b)(1). It is not possible to reasonably segregate meaningful portions of the withheld pages for release. A brief explanation of the applicable sections follows:

Section 1.2(a)(1) of EO 13526, provides that information shall be classified TOP SECRET if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security.

Section 1.2(a)(2) of EO 13526, provides that information shall be classified SECRET if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

Section 1.2(a)(3) of EO 13526, provides that information shall be classified CONFIDENTIAL if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

Section 1.4(c) of EO 13526, provides that information pertaining to intelligence activities, intelligence sources or methods, and cryptologic information shall be considered for classification protection.

In addition, information has been withheld that would result in an unwarranted invasion of the privacy rights of the individuals concerned, this information is exempt from the public disclosure provisions of the FOIA per Title 5 U.S. Code 552 (b)(6).

Additionally, information has been sanitized from the records as the release of the information would reveal sensitive intelligence methods. This information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(7)(E) of the FOIA. The significant and legitimate governmental purpose to be served by withholding is that a viable and effective intelligence investigative capability is dependent upon protection of sensitive investigative methodologies.

The withholding of the information described above is a total denial of your request. This denial is made on behalf of Major General Stephen G. Fogarty, Commanding, U.S. Army Intelligence and Security Command, who is the Initial Denial Authority for Army intelligence investigative and security records under the Freedom of Information Act and may be appealed to the Secretary of the Army. If you decide to appeal at this time, your appeal must be post marked no later than 60 calendar days from the date of our letter. After the 60-day period, the case may be considered closed; however, such closure does not preclude you from filing litigation in the courts. You should state the basis for your disagreement with the response and you should provide justification for reconsideration of the denial. An appeal may not serve as a request for additional or new information. An appeal may only address information denied in this response. Your appeal is to be made to this office to the below listed address for forwarding, as appropriate, to the Secretary of the Army, Office of the General Counsel.

Commander
U.S. Army Intelligence and Security Command
Freedom of Information/Privacy Office (APPEAL)
4552 Pike Road
Fort George G. Meade, Maryland 20755-5995

Additionally, we have been informed by the Central Intelligence Agency (CIA) that their information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(1) and (b)(3) of the FOIA. Exemption (b)(3) pertains to information exempt from disclosure by statute. The relevant statute is Central Intelligence Agency Act of 1949, 50 U.S.C. §403, as amended, e.g., Section 6, which exempts from the disclosure requirement information pertaining to the organization, functions, including those related to the protection of intelligence sources and methods, names, official titles, salaries, and numbers of personnel employed by the Agency.

The withholding of the information by the CIA constitutes a denial of your request and you have the right to appeal this decision to the Agency Release Panel within 45 days from the date of this letter. If you decide to file an appeal, it should be forwarded to this office and we will coordinate with the CIA on your behalf. Please cite CIA #F-2010-00777/Army #681F-09 assigned to your request so that it may be easily identified.

In addition, we have been informed by the Defense Intelligence Agency (DIA) that their information is exempt from public disclosure pursuant to Title 5 U.S. Code 552 (b)(3) of the Freedom of Information Act (FOIA) and 10 U.S.C. § 424.

The withholding of the information by the DIA constitutes a denial of your request and you have the right to appeal this decision directly to the DIA. If you decide to file an appeal, it should be forwarded to the Director, Defense Intelligence Agency, Attention: DAN-1A, FOIA, Washington, DC 20340-5100. Please cite DIA Case #CONF0026-2010 assigned to your request so that it may be easily identified.

Additionally, we have been informed by the National Security Agency (NSA) that portions of their information has been sanitized from the records pursuant to the exemptions listed below:

5 U.S. Code 552(b)(1) – The information is properly classified in accordance with the criteria for classification in Section 1.4 of Executive Order 13526.

5 U.S. Code 552 (b)(2)

5 U.S. Code 552(b)(3) – The specific statutes are listed below:

50 U.S. Code 402 note (Public Law 86-26 Section 6)
50 U.S. Code 403-1(i)
18 U.S. Code 798

The initial denial authority for NSA information is the Director Associate Director for Policy and Records. Any person denied access to information may file an appeal to the NSA/CSS FOIA/PA Appeal Authority. The appeal must be postmarked no later than 60 calendar days of the date of the initial denial. The appeal shall be in writing to the NSA/CSS FOIA/PA Appeal Authority (DJP4), National Security Agency, 9800 Savage Mill Road, STE 6248, Fort George G. Meade, Maryland 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS FOIA/PA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent unusual circumstances.

There are no assessable FOIA fees.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651, or email the INSCOM FOIA office at: usarmy.meade.902-mi-grp-mbx.inscom-foia-service-center@mail.mil and refer to case #681F-09.

Sincerely,

Joanne Benear
Chief
Freedom of Information/Privacy Office

Enclosure

~~TOP SECRET~~ ~~NOFORN//X1~~

(FOUO) ANNUAL COMMAND HISTORY

U.S. ARMY INTELLIGENCE AND SECURITY COMMAND

FISCAL YEAR 2001

History Office
Office of the Chief of Staff
Headquarters, U.S. Army Intelligence and Security Command
Nolan Building
8825 Beulah Street
Fort Belvoir, Virginia 22060-5246

30 September 2002

DERIVED FROM: MULTIPLE ~~SOURCES~~
DECLASSIFY ON: ~~X1~~
DATE OF ~~SOURCE~~: 30 September 2001

TABLE OF CONTENTS

Captured War Criminal Declassification Effort

Army Attaché Management

Impact of AG Transformation on the Field Support Center Activities

(b)(1),(b)(3) Per CIA

Challenges to the Field Support Center

Deployment per Diem

Accident Statistics

Closure of the Army National Capital Region (ANCR) Civilian Personnel Operations Center (CPOC)

Civilian Personnel Changes

Drug Testing

Security Clearance Processing

INSCOM Investment Strategy

FY04-09 POM Strategy

Mail Protection

Wearing of the Beret

INFORMATION AND SYSTEMS Chpt 3 pp 22-26

Transfer of Billets

Overview of Information Arena

Foreign Language Technology Website

501st Network Operations Center Consolidation

Headquarters Networks

Information Dominance Center (IDC) Portal

Viruses

Technology Support Element

Mandatory Deployment of Systems Management Server (SMS)

OPERATIONS Chpt 4 pp 27-52

Unified Cryptologic System

CIA Commendation

Aerial Exploitation

Information Warfare in the Field

Greater Computer Access

Conviction of George Trofimoff

Offensive CI Operations

Army's Relationship to the NRO

Status of SAEDA in Europe

September 11 Legal Policy Changes

Intelligence Oversight Issues

MASINT in Europe

(b)(1)(b)(3) Per NSA

Pre 9/11 Support to Counter Terrorism

MDITDS/Blackbird Database

Army CI Center

NGIC's Reach to the Field

SPO Activities

TAREX Activities

Polygraph Program

TROJAN

EAC IO Requirements

501st Special Operations Concepts

9/11 Search Support

Operation END GAME

Combat Development Target

Deployment of IOWA

Smugglers

MASINT Breakthrough

USN EP-3 Crisis

MRSOC Role

Significant IIR

CI Support to Force Protection

Second Generation Computer

(b)(1)(b)(3) Per NSA

PALMETTO SHIELD/GHOST

NGIC Team Visit

(b)(1)(b)(3) Per NSA

Bad Aibling Coverage

Asian Studies Detachment

(b)(1)(b)(3) Per NSA

500th CI Detachment

902d MI Group

704th MI Brigade

116th MI Group

115th MI Group

LIWA

500th MI Group

501st MI Brigade

INTRODUCTION

(U) *The following are excerpts from a statement delivered by Major General Keith Alexander, CG INSCOM, to the House Permanent Select Committee on Intelligence (November 14, 2001):*

****

(U//~~FOUO~~) INSCOM's transformation to meet the growing challenges of an asymmetric, transnational threat began in earnest prior to 11 September. The attack on the *USS Cole* highlighted the need for greater focus on actionable counterterrorism intelligence. USCINCCENT asked the Chairman, Joint Chiefs of Staff, to support development of a program to "get out in front" of the CT threat using the Information Dominance Center, at INSCOM. In December, 2000, the Chief of Staff of the Army agreed with this tasking and directed INSCOM to take on these operations. INSCOM intensified that focus during a February 2001, Commanders' Conference, which assembled the Brigade Commanders of the previously mentioned units. The conference was devoted to envisioning a revised concept of INSCOM's mission and capabilities. In the end, the conferees recognized the need for a new methodology to transform the entire Command as it confronted the asymmetric threats, while, at the same time, meeting the challenges of providing operational intelligence in the Army's Transformation.

(U//~~FOUO~~) n the past, INSCOM units generally conducted their respective missions as discrete entities. The INSCOM Headquarters performed personnel administration, logistics, resourcing, planning, and programming functions, but did little in the way of Command-wide mission management, synchronization, on focusing these disparate units against a specific intelligence problem. The new challenge was to optimize the efforts and effects of a worldwide, multi-discipline intelligence organization.

(U) ~~(S//NF)~~ The significant change INSCOM made is both physical and mental-transforming the MACOM headquarters into an organization focused on unifying the intelligence operations of our subordinate units, and ensuring a common view in the battle against terrorism. The intellectual and technical capabilities of the NGIC and the SIGINT Brigades link with the operational expertise of the Theater Brigades, the 902d MI Group, LIWA, and our Special Missions Units. Thus CI/HUMINT, SIGINT, Science and Technology, and operations are woven together, along with the Information Operations efforts, into a synergy that ensures the best minds and intelligence tools are harnessed, via the INSCOM Information Dominance Center (IDC) to support commanders. The goal is to prosecute the Army's and Nation's toughest challenges of Counterterrorism (CT), Counternarcotics (CN), Counterintelligence (CI), and Computer Network Operations (CNO) in a comprehensive, integrated, collaborative manner. All in one Command, each in an agile and optimized fashion.

(U//~~FOUO~~) From February to June 2001, INSCOM commanders and staff completed much of the preliminary work for instituting a transformed organization. We identified the requisite enablers: people,

resources, policy changes, databases, and communications improvements necessary to ensure command-wide collaboration and synchronization.

~~(S/~~ ~~/NF)~~ In June, INSCOM entered into a formal agreement with the National Security Agency, which allowed us to access to specific classified databases and to receive live communication feeds from (b)(1)(b)(3) Per NSA This was an unprecedented step by the DIRNSA, for which he and NSA should receive full credit! The summer was spent exploiting data bases and live "metadata" to identify terrorist networks, wile simultaneously developing the tactics, techniques, and procedures of running an Information Dominance Center (IDC). Concurrently, we established the operational procedures for ensuring the full engagement of the entire command.

(U) Accelerated Transformation: Post-11 September

~~(S/~~ ~~NF)~~ The next phase of INSCOM's transformation incorporated the most significant enhancements. On 14 September, INSCOM deployed 10 analysts to NSA to form the IDC-Meade element to assist the CT Office of Primary Interest. Additionally, 2 linguists were attached directly to the CTOPI. The intent was to augment NSA's on-going analytic efforts by leveraging the IDC's processing capabilities. With the continued support from NSA and analytic engagement with DIA, CIA, and the FBI, the INSCOM Information Dominance Center (IDC) captured the elements of data storage, data feeds, data acceleration, and robust analytic tools in dramatic ways. This resulted in

(b)(1)(b)(3) Per NSA

(U) ~~(S//NF)~~ In order to get real-time information to the warfighter and ensure Command-wide collaboration, we established a web-based technology portal on which we post our counterterrorism analytic exchanges. The portal enables an interactive link from INSCOM to our Brigades, the Army Operations Center at the Pentagon, the Army Service Component Commands, Defense Intelligence Agency's Joint Terrorism Analysis Center, Joint Commands - most notably CENTCOM, and National Agencies. The intellectual energy of the entire Command is harnessed and focused every day through the use of this portal and worldwide, classified, video tele-conference, during which we synchronize the intelligence operations of each of our units in the fight against terrorism.

****

CHAPTER ONE

MISSION AND ORGANIZATION

Headquarters Reorganization. (U/~~FOUO~~) At the January 2000 offsite, the leadership from the INSCOM staff met for the purpose of taking the command's strategic plan one step further and looking at what would allow the organization to reach its 5-year objectives. What came out of the meeting was the FY 00/01 INSCOM Performance Plan. One of the plan's objectives that was raised and approved by MG Noonan, CG INSCOM, was to establish an executive working group to review the headquarters structure and functions. Unlike recent studies such as the one performed by Mystech Associates in 1997, this was to be done in house and at little cost to the command. General Noonan wanted to know what was needed organizationally to accomplish the command's long-term goals. He went on to emphasize that he was not wedded to the past. More specifically, the Commanding General asked the working group to address the following questions: Is the current G-structure adequate? Are there functions being performed that are no longer needed? Can other functions and organizations be streamlined for the sake of efficiency? The working group was also to look at possible savings that the Command Group could redirect to areas of emerging priorities (LIWA, IOC, etc.). Finally, the working group was to be mindful that the command had a man-power survey coming up. If there were areas of vulnerability, then realignment of spaces could be made up front.

(U/~~FOUO~~) The 12-person working group, chaired by a representative from DCSRM, set out to conduct a functional analysis of the headquarters. Besides input from the various staff elements, the members of the working group conducted interviews with key members of the staff. In June 2000, the working group issued a report with the following conclusions: Consolidate major compliance and oversight processes to achieve greater focus and coordination. Consolidate System Integration and G-6 into one information management/technology organization. Reduce the complexity of the G3 organization. Force management and system acquisition should be realigned into a single element. The Deputy Commander and Chief of Staff positions should be realigned to function similar to an Army Division. INSCOM should establish a MACOM CPAC. Finally,

consolidate a number of functions such as safety and training.

(U//~~FOUO~~) The working group presented General Noonan with four options for restructuring the headquarters: The first was basically the same G-staff structure already in place. Options 2 and 3 created subordinate deputies under the Commanding General. These would be called Deputy for Support (including Personnel, Contracting, Resource Management, and Logistics) and Deputy for Intelligence Operations and Technology. Option 2 would further divide the Deputy for Intelligence Operations and Technology into two directorates: one for operations and systems acquisition and the other for information management and telecommunications. The only difference for Option 3 was that the Deputy for Intelligence Operations and Technology was further broken down into three directorates: operations and security; futures (systems acquisition); and information management/technology. Option 4 would be the most far-reaching of the proposals. The staff would be divided between a Deputy for Support, a Deputy for Operations, Security & Systems Acquisition, and a Deputy for Information Management/Technology. (Ironically, following a high-level, high cost study of its own, NSA would emerge with an organizational restructuring much like that shown in Option 4.)

(U//~~FOUO~~) However, unexpected events would interfere with the planning process. Anticipating his appointment as the new DCSINT, General Noonan hesitated to make a decision that his predecessor would have to live with. Consequently, the reorganization process was placed on hold. Because naming of a new commander was delayed until early 2001, the whole issue lay dormant. In the interim, (b)(6) COL [redacted] the Chief of Staff, coordinated the original recommendations among the staff and amended where appropriate.

(U//~~FOUO~~) In March 2001, BG Alexander, the new INSCOM CG, was briefed on the various restructuring options and chose to maintain the G-staff. He did not want to become so dissimilar from the rest of the Army that INSCOM was not recognized as an Army command. The more that INSCOM looked like the warfighters, the more they could identify with the command. General Alexander proceeded to appoint COL [redacted] (b)(6) to meet with the staff and pare down the recommendations. What emerged in July 2001 was a three phase implementation

process. All three phases would run simultaneously and were scheduled to be completed in 4 months, 8 months, and 12 months. Tiger Teams would be used to complete the process. By 1 October, the following major changes were to be completed: establishment of a Command Information Cell, development of a Compliance Process, analyze the establishment of an INSCOM CPAC, transfer the commercial process from G4 to G3, transfer of COMSEC oversight from G2 to G6, transfer of CCP (Consolidated Cryptologic Program) from G3 Army Cryptologic Office to DCSRM, and define the G3 Counterintelligence Office. Again, unforeseen events disrupted the planning process. After September 11, the Chief of Staff decided to proceed with only phase one. It was felt that to do more would be too disruptive for a staff focused on a war against terrorism.

Coming of Multi-Component Contingency Support Brigade (MCSB). (U) The following is an excerpt from an article by (b)(6) LTC [redacted] (Utah National Guard): The Intel XXI Study (also known as "The Hall Study") identified a number of unique, one-of-a-kind military intelligence assets that have the potential of spanning all echelons of the Army. The idea of a Multicomponent Contingency Support Brigade (MCSB) developed from this study. The mission of the MCSB is to provide increased full-spectrum capabilities at both echelons above corps (EAC) and echelons corps and below (ECB). The concept is to "pool" these unique capabilities to support the Total Force and to provide tailored packages of specific skills from this pool of broader resources. These tailored packages would be modular and flexible in order to meet the specific needs of the Total Force.

(U) The vision for the MCSB was further enhanced and refined in January 2000 during the MI Functional Area Assessment (FAA) when the Vice Chief of Staff for the Army (VCSA) approved the recommendation to develop a Force Design Update (FDU) for the MCSB. That decision included establishing an MCSB to 'support Army contingency operations with unique, one-of-a-kind capabilities.' The approved recommendation also assigned the MCSB to US Army Intelligence and Security Command (INSCOM) with operational control to US Forces Command (FORSCOM). The reason for this arrangement was to maintain the existing training relationships between INSCOM units and the current elements designated for the MCSB, while giving FORSCOM the ability to "plug and play" the pieces of the MCSB when and where they were most needed.

(U//~~FOUO~~) The initial force design included the following: the 300th MI Brigade (Linguist) as the headquarters element with representatives from the Active Component, Army National Guard, and Army Reserve. An electronic warfare unit formed from two Army Reserve units– the 323d MI Battalion and the 368th MI Battalion. An Active Component linguist unit designated to provide "first-in" deployment assets. Nine MI linguist companies pulled from

the Reserves along with six National Guard linguist battalions. The 203d MI Battalion, an existing multi-component unit in support of the National Ground Intelligence Center, was included. Finally, the 96Hs (Common Ground Station Operators) from the Joint Surveillance Target Attack Radar System were also made a part of the brigade.

First Multi-Component MI Unit. (U//~~FOUO~~) On 16 June 2001, the first military intelligence multi-component unit was activated–the 203d MI Battalion at Aberdeen Proving Ground, Maryland. The multi-component concept began in 1997 when INSCOM was directed to make personnel cuts while still maintaining its mission. LTC [redacted] then commander of the 203d, and his staff came up with the multi-component plan. (The battalion already had a working relationship with two Reserve companies.) The process towards the activation was not an easy one and required drawdown and inactivation of the 203d by the Active Army as well as several companies in the Reserves. This restructuring allowed for the residual elements to fit into the new multi-component battalion activated on 16 June 2001. The battalion consisted of one integrated active/reserve company and two reserve companies (authorized strength was 253). The 203d had the unique mission of providing warfighter commanders with technical intelligence on foreign equipment and weapons systems. The 203d trained on foreign weapons, equipment, and both wheeled and tracked vehicles and participated in opposing forces operations at the National Training Center, Fort Irwin, California.

(b)(6)

INSCOM Performance Plan. (~~U//FOUO~~) At the January 2001 leadership offsite [redacted] the Command Group and staff leadership tackled the creation of a FY 00/01 Performance Plan. Using INSCOM's 1999 Strategic Plan, which covered goals for the next 5-6 years, the group created an annual plan to accomplish the long-term goals (some 36 initiatives). It also satisfied the demands of a newer requirement, the Government Performance and Results Act that encouraged an on-going planning process.

(b)(1),(b)(3) Per CIA

Strategic Goals. (U//~~FOUO~~)

1. Provide Actionable Intelligence to the Army Operations Center and the Army Service Component Commanders.

Strategic Objectives

1.1 Evolve the IDC CONOPs and architecture in concert with Army Leadership.
1.2 Develop doctrine and TTP for identifying, processing and disseminating actionable intelligence.
1.3 Demonstrate INSCOM capabilities to the Army leadership and the Intelligence Community.

2. Ensure INSCOM's Vision, Mission, and EAC Concept of Intelligence and Information Operations are Embedded into Army and Joint Doctrine.

Strategic Objectives

2.1 Secure acceptance by Senior Leaders of Army, DOD and the Intelligence Community.
2.2 Implement transformation concept into CONOP concurrently with Senior Leadership acceptance.
2.3 Identify relevant policies and propose changes/additions within 6 months of implementation.
2.4 Develop and implement plans to advance INSCOM's mission, vision, and capabilities NLT FY02.
2.5 Continuously revalidate, refine, and review intelligence and Information Operations requirements.

3. Identify and Establish Relationships and Agreements with DOD, the Intelligence Community, and Inter-Agencies to Advance INSCOM and Army Vision and Mission.

Strategic Objectives

3.1 Identify strategic partners by MSC, staff element, and discipline.
3.2 Define roles, responsibilities, and relationships and review annually.
3.3 De-conflict and synchronize INSCOM operations with Joint, Combined, and National level Intelligence Agencies/Organizations.
3.4 Formalize agreements as appropriate and review biennially.
3.5 Implement a strategy to advance INSCOM's vision and mission NLT FY02.

4. Identify, Exploit, and Sustain Leading Edge Technology.

Strategic Objectives

4.1 Establish and empower a coordinating office/technology board as the focal point for all future technological support requirements.

4.2 Actively participate in the Combat Development process.
4.3 Interface with industry, academia, and science and technology centers to leverage emerging technology.
4.4 Develop tactics, techniques, and procedures for identifying, exploiting, and sustaining leading edge technology.

5. Recruit, Train, and Retain a High Performance, Empowered Workforce.

Strategic Objectives

5.1 Attract and retain high performance personnel.
5.2 Establish developmental programs to sustain a quality workforce, and promote quality of life and wellness of the command.
5.3 Meet personnel retention quotas.
5.4 Ensure equity and fairness in the recognition and promotion of excellence.
5.5 Identify and reduce roadblocks and impediments to recruiting and retaining required personnel.

6. Resource and Organize the Command to Provide Real Time Intelligence, Security, and Information Operations Support to the Army Operations Center and the Army Service Component Commander.

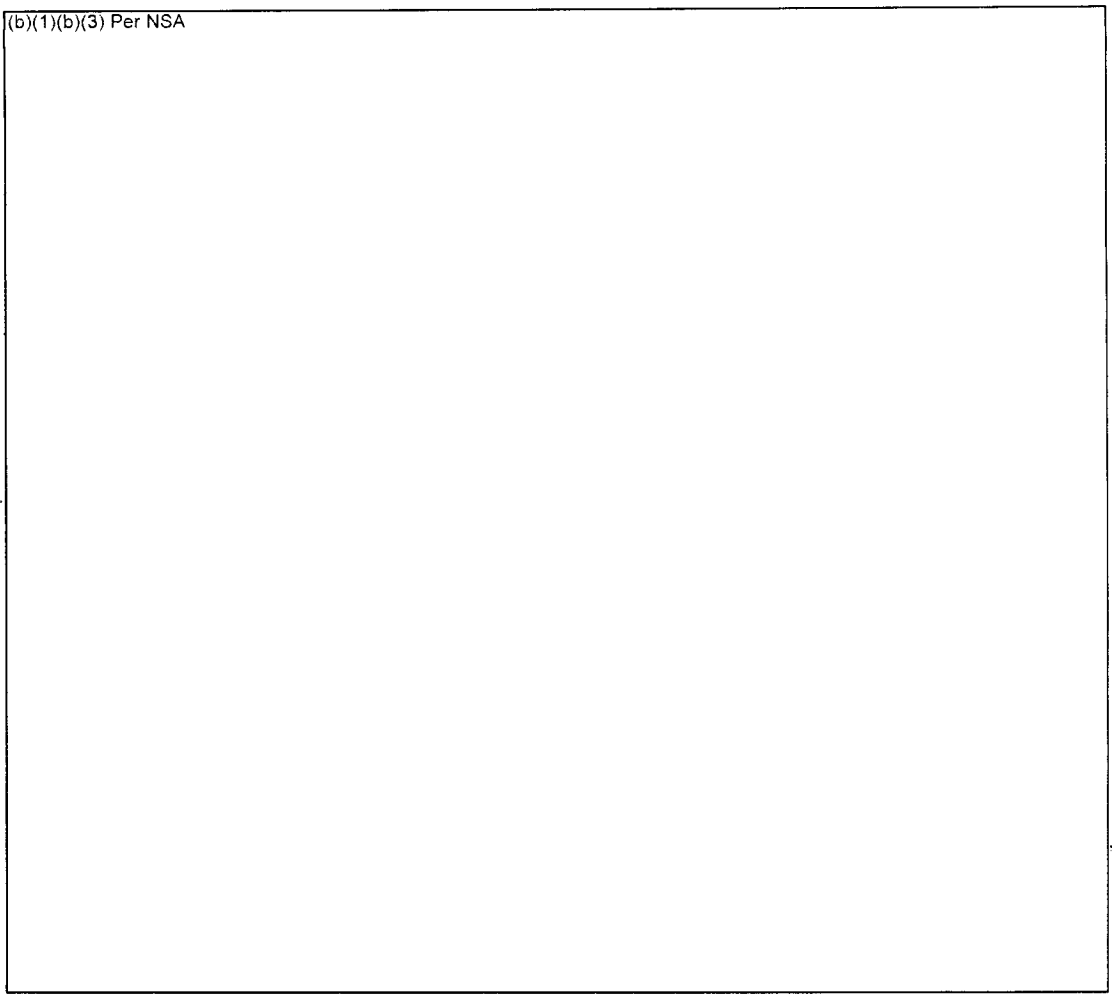
Strategic Objectives

6.1 Continually assess adequacy of command resources and structure to meet requirements.
6.2 Realign command resources to enable a knowledge-based, prediction oriented intelligence process responding to commander driven requirements.
6.3 Identify and leverage potential external sources of resourcing (funding and personnel).
6.4 Provide quality facilities and state-of-the-art Information Technology infrastructure to sustain INSCOM's people, equipment, organization, and mission.

(b)(1)(b)(3) Per NSA

~~TS~~

(b)(1)(b)(3) Per NSA



Standing Up of the Information Dominance Center (IDC). ~~(S//NF)~~ The IDC was established 2 years ago by LIWA. However, during the 4th Quarter, FY 01, the IDC evolved into becoming a "provisional" major subordinate command of the INSCOM. This change came as a result of how the IDC performed operations. The Information Dominance Center evolved into a congregation of powerful search and analytical tools, simultaneously coupled to available databases (IMINT, HUMINT, and SIGINT), and attached to a front-end SIGINT collection site. On 3 August 01, the National Security Agency assigned the SIGINT Designator

(b)(1)(b)(3) Per NSA [redacted] to the IDC. (This was a part of General Alexander's vision of offering "one-stop intelligence and information operations shopping.") The change in operations also led to organizational changes. The Commander, LIWA, was dual hated as the Commander, INSCOM IDC. Other entities wrapped into the IDC were the Intelligence Operations Center,

Futures Center, and Cyber Warfare Center. (The Intelligence Operations Center expanded its mission to provide Army-wide real-time Indications and Warnings (I&W) of count-terrorism, counterintelligence, information operations, and counter-narcotics supporting the total Army's overall "Force Protection.") The IDC possessed the necessary skilled IO and intelligence professionals along with software, hardware, and communications architectures to allow for worldwide synchronization and engagement of IO, IO-related, and focused-intelligence operations.

CHAPTER TWO

PERSONNEL, SECURITY, LOGISTICS, *Etc.*

MASINT Training. (U/~~FOUO~~) The MASINT Branch, G3, HQ INSCOM undertook a training initiative to ensure that warfighters would have greater access to MASINT scientific and technical intelligence. In October 1977, it began to offer the MASINT Basic Collector's Pilot Course; this was followed up with an Immediate Course and the MASINT Basic Analysis Training Course. These courses were directed at several different audiences. The first were to those MASINT specialists (civilian/military/Active/Reserve) being deployed. The courses provided an understanding of the MASINT community and how MASINT could be leveraged to meet intelligence requirements and contributed to the personnel's operational efficiency. A second group included members of the Analysis Control Elements, military intelligence commanders, and all the 2s (G2s, S2s, etc.). The purpose was to furnish these key intelligence types with the knowledge on how to fuse MASINT with other intelligence disciplines and how to leverage the systems to support intelligence operations. In FY 1998, 125 personnel had completed the courses; a year later, the total was 401. Formal training was also supplemented with interactive computer-based education including video tapes covering subjects that ranged from basic physics to collection management.

Reserve Status. (U/~~FOUO~~) FY 01 began with 224 allocated Reserve positions; another 19 positions were added for LIWA in the middle of the year, bringing the total to 243. (This did not include an additional 98 undocumented augmentees allocated to the Investigative Records Repository for a special screening and declassification project involving World War II records.) For FY 2001/02, INSCOM was scheduled for a plus up of 50 more individual mobilization augmentees (IMA), bringing the funded total to 293.

Overview of Security Issues. (UNCLASS/~~FOUO~~) Following the end of the Cold War, there were a number of important changes in how security threats against the Government were handled. Overall, the military, intelligence, and security environment became more complex not less so. When the Soviet Union was America's greatest potential adversary, it

was easy to ignore other threats. Once the Berlin Wall came down and the Soviet Union collapsed, the military and the intelligence community were faced with new challenges, such as China. The emergence of the United States as the sole world superpower also compounded the security problem. For instance, many countries that had been subservient to the Soviet Union or had close ties were now free to act independently.

(U) ~~(C)~~ At the same time the Soviet Union was coming to an end, computer technology was beginning to advance at an unparalleed pace. Suddenly security managers were faced with protecting information as opposed to documents, and information proved far more difficult to control. Now security types had to be aware how information was moving inside/outside their organization and by what means (phone, fax, e-mail, etc.). This required the installation of safeguards at critical points in the process. This became a tremendous challenge. The most common security violations facing INSCOM involved technology. For example, the case of an e-mail or a fax improperly classified or being sent over a nonsecure line. To complicate matters, it became easier for a person to make errors and to make them faster. The atmosphere at the major headquarters in which speed was demanded also did not help. And in future all would be compounded as technology continued to develop. For instance, the emergence of hand-held devices that plugged into systems and the use of infra-red waves for communications.

(U) ~~(C)~~ Unfortunately, many of today's security managers were not technologically savy enough to determine policy and to know the vulnerability of systems. For instance 20 years ago, security managers were concerned with double wrapping documents; now its e-mailing around the world. This has left security highly dependent upon a handful of persons with a high-degree of expertise to protect the systems. However, there are an insufficient numbers of such people in the Government to keep security up-to-date. This has led to security policy lagging behind state-of-the-art technology. Personal Digital Assistants (PDA), for example, were out before anyone had a policy on them. There is also a growing concern that even the so- called experts do not have a complete handle on all the potential vulnerabilities. For instance, the only difference between NIPRNET and SIPRNET is that the latter is encrypted, but both are using the same transmittal system. Because of

technology, those inside the system possess so much more access to information than in the past and that information can be captured in a disk and does not require a whole safe full of documents. One person walking out with a zip-drive in a pocket that cannot be searched without a warrant is our biggest threat. Through the years there has been a total break down of the "need to know" as a means of protecting information. A part of that breakdown can be attributed to the access that technology has provided the average member of the staff. SAP's are a part of the answer along with the use of stand-alone computers. Segregating information is another, but this is not a fool-proof system because individuals with sufficient know-how can break through fire walls. As we hire a new generation with increased technology smarts the vulnerabilities will only continue to increase. The bottom line is that as of today the security community remains behind the power curve in addressing these technology changes seriously. Security simply lacks the people with the know-how to do the job.

(U) ~~(C)~~ As the Cold War ended, the United States found itself dealing with more flashpoints. New alliances were formed, some of them with former enemies. How and what kinds of information can be shared? The DCI finally got serious about the whole issue of foreign disclosures in the last year and came out with guidance. For instance, HQDA has taken steps to ensure that INSCOM doesn't invite foreign personnel to the headquarters unless there is a specific reason. The Land Information Warfare Activity also plays a role in security. Its focus is counterintelligence such as having teams evaluate the vulnerability of a particular system. Information gained by LIWA in identifying and evaluating potential problem areas can be used to shape future security policy.

(U//~~FOUO~~) September 11th has brought new awareness of the threat. As a result, the overall security posture will change. Those in the intelligence business and the military will also experience changes in security, but they will not be as dramatic as the rest of the government because the intelligence/defense community is already operating at a higher level.

Contingency Funding. (U//~~FOUO~~) INSCOM continued to be tasked for the Bosnia and Kosovo contingencies. Due to scarce Army resources, it was once again necessary to justify INSCOM contingency requirements. Here, the Budget

Branch, DCSRM (HQ INSCOM) took the lead and was successful in receiving full funding. INSCOM's requirements slightly decreased for Bosnia to $11.5 million and increased for Kosovo to $8.8 million. (Resource requirements exceeding the USAREUR reimbursement were absorbed from internal funding.) INSCOM also received additional contingency funds in the amounts of $698,000 (FCI) for Southwest Asia, $1.056 million (FCI) for Bosnia, and $2.002 million (GDIP) for NGIC, Army Central, and Reserves.

Conversion of Inventory Control Systems. (U/~~FOUO~~) The Mission Stock Record Account (MSRA), which had transferred to the Intelligence Materiel Activity in FY 2000, had for years experienced difficulties with the use of the SARSS-O as an inventory control system. The problem was that SARSS-O was designed for standard items but MSRA primarily dealt with nonstandard, commercial off-the-shelf items. In early FY 2001, the G4 (HQ INSCOM) approved MSRA converting to the Inventory Control, Analysis, and Reporting System (ICARS). The conversion was considered a success.

Technical Surveillance Countermeasures (TSCM) Support. (U/~~FOUO~~) During FY 2001 the Intelligence Materiel Activity (IMA) continued to support the TSCM activity. In addition to providing acquisition and maintenance support for Army TSCM, IMA also provided these services plus training, testing, and development support for a growing number of non-Army agencies and activities. They included the Department of Energy and the Marine Corps.

Logistical MOUs/MOAs. (S) The ACofS, G4 had a record of 170 Inter/Intraservice Support Agreements and logistical MOUs/MOAs for INSCOM units both CONUS and OCONUS. The support agreements involved 85 installations, 61 of which were in CONUS and 24 OCONUS. For example, there was a memorandum of agreement between the INSCOM G4, SOUTHCOM, CECOM 12WD, and USAREUR to define the responsibilities for providing on-site electronic maintenance support for the TROJAN Air Transportable Electronic Reconnaissance System (b)(1)(b)(3) Per NSA integration and installation assistance with the TROJAN Classic upgrade to MCO3; and site support to TROJAN systems (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

Tactical Exploitation of National Capabilities (TENCAP). (U) ~~(S)~~ As part of the TENCAP effort, the Tactical Exploitation System (TES) was prepared for fielding by the 297th MI

Battalion at Fort Gordon. The system was in a HMMWV configuration which was to be upgraded to Wolf Coaches in its Final Operational Capability in FY 2002. Due to subcontractor slippage, system delivery was delayed and TES MAIN did not arrive at Fort Gordon, Georgia, until September 2001. At the fiscal year's end, fielding activities were still in process.

(~~S~~ -)

(b)(1)(b)(3) Per NSA

Gordon Facilities. (U/~~FOUO~~) The Gordon Regional Security Operations Center (GRSOC) was housed in Building 24701 (Back Hall), a two-story structure with a partial basement constructed in 1988. It had two interior open courtyards, which were accessible only from the inside first floor, plus a secure door for loading, unloading, and storage of all items shipped into or out of Back Hall. The building's footprint was approximately 79,200 square feet with approximately 50,900 square feet usable workspace for mission and mission support systems. Back Hall was planned and designed to accommodate a Satellite training mission, but was assigned to INSCOM in May 1995 for the GRSOC (operational, training, and administrative functions). In 1995, several construction projects totaling approximately $1.2 million, improved the HVAC and electrical systems, replaced and modernized the existing telephone system, and installed an uninterrupted power system. During FY 1998, three construction projects were completed that provided redundant electrical switchgear and transformers. In FY 1999, a new roof and an addition to Back Hall were added; the addition increased mission space by 1,250 square feet. In FY 2000/2001 the electrical system was again upgraded with Transient Voltage Surge Suppression (TVSS).

(U/~~FOUO~~) The Joint Language Center and the Headquarters, 116th MI Group moved from Building 21721 into Building 36708 the "Old" O'Club in November 2000. The Building 36708 was then renovated in just 8 weeks. Building 21721 underwent a 12-month $2.1 million HVAC and Electrical upgrade. Plans called for the top two floors of

the converted barracks to become a SCIF and to house J-3 classified training and the Navy Master Language Course. The first floor would serve the Headquarters, 116th MI Group.

New Home for NGIC. (U/~~FOUO~~) On 21 September 2001, the Nicholson Building (final price tag: $46.2 million dollars) was dedicated in honor of LTC Arthur D. Nicholson. (Nicholson, a member of the US Military Liaison Mission was shot and killed on 24 March 1985 while on a routine mission. He has been called "the last casualty of the Cold War.") The 256,000 square foot facility at 2055 Boulders Road, Charlottesville, Virginia, will serve as home to the National Ground Intelligence Center and will consolidate NGIC employees previously located at six rental properties within the Charlottesville area. In addition, some employees of NGIC's element at the Washington Navy Yard, District of Columbia, were also relocated to the new building.

Captured War Criminal Declassification Effort. (U) Following World War II, the US Government, including military intelligence, collected a large amount of records and information on Nazi war crimes and their perpetrators. As a result of the collapse of the Soviet Union, and their releasing records on the Nazi era, there was an increased interest in the subject, especially questions regarding the fate of Nazi-seized valuables and properties. To address these growing concerns, Congress passed the Nazi War Crimes Disclosure Act of 1998 that mandated the identification of still-classified records related to war criminals of World War II Axis governments. Once identified, they were to be reviewed and released to the American public. The Army's Investigative Records Repository at Fort Meade, Maryland, alone held 11,400 reels of microfilm representing more than 1 million documents. As commander, MG Robert Noonan committed INSCOM to completing the project within a year. (One expert estimated that manual review would take 181 man years to complete.) To meet its deadline, INSCOM turned to Sherikon, Inc., a reseller of document imaging solutions and Kofax Ascent Capture software, a high-volume document capture application that was coupled with Wicks and Wilsor high-speed microfilm scanners. Using 150 soldiers drawn largely from the 902d MI Group and 704th MI Brigade, the declassification team worked 6 days a week, 24 hours a day. The project was completed ahead of schedule and about 16,000 files related to Nazi-war crimes were identified.

(b)(1) & (b)(3) PER DIA

[redacted]

All total, the division supported [redacted] Army personnel assigned to [redacted] embassies worldwide. During the year, there was an ongoing effort to ensure that [redacted] remained a valid MI WO MOS. At the same time, the Field Support Center undertook several important initiatives: re-certified [redacted] maintained close relationship with the Soldier Support Center at Fort Jackson, South Carolina, to reconfirm the career path and promotions of NCO's; and staffed AR 611-60 that allowed the Field Support Center to recruit MI linguists for hard-to-find assignments.

(b)(1) & (b)(3) PER DIA

Impact of AG Transformation on the Field Support Center Activities. ~~(S)~~ The Adjutant General Transformation announced by the DCSPER of the Army had a number of impacts upon the Field Support Center. First, it was determined that the Military Personnel Center Chief had to be civilianized in order to maintain long-term continuity in essential knowledge and technical skills. Secondly, the coming of a "paperless" Army meant that individual soldiers would be given more overview of the management process pertaining to their careers. [redacted]

(b)(1)

[redacted]

(b)(1),(b)(3) Per CIA

(b)(1),(b)(3) Per CIA

(C)

(b)(1)

Deployment per Diem. (U) The FY 00 National Defense Authorization Act authorized "high-deployment per diem," and established the requirement to track soldiers' deployed and non-deployed time away from home. Congressional intent was to penalize all the services and their components for high deployment, and to reduce the time soldiers' spent away from home, thereby improving morale and quality of life. The Army's requirement to begin tracking started on 1 October 2000.

Accident Statistics. (U) For FY 01, INSCOM experienced 41 recordable accidents at a cost of $292,508, primarily sports and POV related.

Closure of the Army National Capital Region (ANCR) Civilian Personnel Operations Center (CPOC). (U) The closure of the ANCR CPOC led to the transfer of INSCOM Defense Civilian Intelligence Personnel System to the West CPOC at Fort Huachuca. At the same time, the Civilian Personnel Advisory Center was also transferred from the Personnel and Employment Services-Washington in the Pentagon to the Fort Huachuca CPAC. The transfer was completed by 6 October 2001. Plans called for the Fort Huachuca CPAC to establish forward based servicing at Fort Belvoir, Charlottesville, Virginia, and at Fort Meade, Maryland, to support local INSCOM elements.

Civilian Personnel Changes. (U) The transition from the Personnel Process Improvement (PPI) to the Modern Defense Civilian Personnel Data System (MODERN DCPS) took place at

the Army National Capital Civilian Personnel Operations Center in April 2001. This was part of the final phase to bring the military departments under one personnel processing system. By the close of the fiscal year, all CPOCs worldwide would be under the new system. Also in FY 01, the Inventory Based Recruiting (IBR) was put into place. When the CPOC received the recruit action all resumes that match the occupational series, lowest acceptable grade, and geographical location were entered into the applicant pool. (A resume would have to be entered into the system only one time.) The resumes of the applicant were then matched against the required and desired skills submitted by the manager. The resumes that matched all the required skills and the greatest number of desired skills were referred for consideration. A new award policy was also implemented on 1 October 2000. Commanders/Staff Heads could expend up to $2.5 percent of base pay but no more than 40 percent of the employees could receive cash performance awards and no more than 10 percent could receive Quality Step Increases or Exemplary Performance Awards. Although INSCOM had 14 man-years allotted to its intern program only 3 were actually on board at the end of the fiscal year due its ability to place personnel and to security processing delays.

Drug Testing: (U) Random drug testing for INSCOM civilian employees was implemented on 1 September 00. The program was command-wide on a monthly basis and was designed to meet DOD's requirement for testing of 50 percent of the command's occupied testing designated positions that numbered approximately 1850. Despite the interruption of testing due to 9/11, INSCOM still was able to test approximately 49 percent (904) of its pool. In addition, INSCOM conducted 222 pre-employment tests; of these entry tests, none were known to be positive.

Security Clearance Processing. (U) At the end of the FY 01, over one hundred tentative job offers had been made for INSCOM open civilian positions with 40 to 45 percent awaiting a security clearance. In September 2001, an interim clearance policy was put into place to accelerate the process for new employees. An interim clearance could be granted (given no derogatory information) following the initial National Agency Check (NAC) or a favorable NAC within the last 10 years or a SECRET clearance within the last 10 years. Those with no previous investigation could be assigned unclassified duties.

INSCOM Investment Strategy. (U) The INSCOM Investment Strategy (I2S) broke down a mission program into quantifiable strategies, and also identified the benefit to the warfighter. The strategies were then prioritized to ensure the most critical requirements were being resourced. The I2S was used as the basis for the development of INSCOM program submissions. A key result of the process was the determination of impacts for potential funding reductions or increases. This process required total staff involvement and ensured a balanced program was identified to include items such as equipment, maintenance, and automation. It also identified those requirements theater commanders addressed during the Integrated Priority List process.

FY 04-09 POM Strategy. (U) In July 2001, the Resources Management and G3 staffs' new strategy for the FY04-09 Army POM was approved for implementation. The objective was to increase INSCOM's market share of available Army resources. The new initiative changed several HQ INSCOM business processes for programming and budgeting, empowering the G-staff to take "ownership" for Management Decision Packages (MDEP) under their purview. The major changes were designating, by name and staff section, functional mangers for the existing 27 MDEPs of the command and also for 15 new MDEPs that have potential to provide additional resources; providing all MDEP managers training on the PPBES, Army POM development process and INSCOM Investment Strategy; adoption of a standard briefing to describe INSCOM's part of each MDEP, to be used for communications with HQDA. The intent of the new strategy was to increase sources of funding, better align INSCOM missions with standard Army programs, and establish or improve rapport between HQDA MDEP mangers, INSCOM MDEP mangers, and major subordinate command counterparts.

Mail Protection. (U/~~FOUO~~) The Headquarters Mail and Distribution Office operated the AS&E X-Ray inspection system on a daily basis to screen all incoming mail pieces/parcels brought into the Nolan Building from external sources for potential explosive devices. The AS&E MICRODOSE® X-Ray inspection system with BackScatter® technology was designed to detect plastic explosives.

Wearing of the Beret. (U) On 14 June 2001 (birthday of the US Army), soldiers (officers, warrant officers, and

enlisted) who were not authorized to wear the tan, green, or maroon berets donned the black beret.

CHAPTER THREE

INFORMATION AND SYSTEMS

Transfer of Billets to USAIC. ~~(TOUO)~~ As a result of the larger MI "Unified Proponency" effort going on, the DCSINT (LTG Kennedy) and CG, INSCOM (MG Noonan) agreed in early 2000 that 61 billets (representing eight combat development regulatory-based requirements) should be transferred from the control of INSCOM to USA Intelligence Center at Fort Huachuca, Arizona and thus solve a problem that had existed for 15 years. It was simply a matter of putting all combat development spaces in one basket. The CG, INSCOM, being a MACOM, served as the specified and functional proponent material developer (AR 5-22) and the organization through which ODCSINT executed its requirements. (There were other requirements, such as INSCOM being designated the Army's Service Cryptologic Element, etc.) At the same time, the CG USAIC&FH served as the branch proponent. (The location of most of the transferred spaces would not change from the Nolan Building at Fort Belvoir, but rather only the control would pass to USAIC.) These spaces would continue to focus on echelon above corps issues for the most part. However, despite the transfer, a number of fundamental problem areas still remained unresolved. In the past, Fort Huachuca had often failed to adequately address EAC architecture, and INSCOM had only done it on a project by project basis. In summary, minimal effort was given to identify the broad range of INSCOM requirements that went beyond a five-year timeline.

Overview of Information Arena (U) ~~(C)~~ Over the last several years, there were several major themes within the G-6 arena. Just 3 years ago, the headquarters was in the process of fielding a LAN system within the Nolan Building that was a combination of ATM and Ethernet. Many had jumped on the ATM wagon when it first came out, but had failed to understand that ATM was not intended for local networks. Rather, ATM was created to work in the "white area" (outside the building and for long distance.) As a result, there were growing complaints from users on how slow their systems were working. The first step in solving the problem was to get rid of ATM and to move exclusively to Ethernet. This proved to be a major milestone in networking. Since then the command took a second step to GIGABIT Ethernet. (The upgrades on IDUN and SIPRNET had

just been completed, leaving only the THOR and NIPRNET to go.) The headquarters also demonstrated the ability to make quantum improvements in networking capabilities. Just 3 months ago, the IDUN was 10 share (that means that everyone was operating at 10 megahertz which led to numerous collisions on the network). This was an example why upgrading must be ongoing. It is interesting to note that LIWA was currently experiencing many of the same problems that the headquarters had to wrestle with 3 years ago—slowdown of the desktop network due to ATM. Erroneously, consumers often believe they have a bandwith problem and go out and purchase too much. In the past, the critical question of whether or not people actually required what they requested was not being asked. As a result, a couple of trunks lines leaving the building are using only 2 percent of their capabilities.

(U//~~FOUO~~) Funding was a key to success if networks were to be systematically upgraded. Because people don't adequately articulate their needs, they often fail to obtain the necessary funding. The bottom line is that the funding cycle must be rigorously followed. To illustrate, over the last three years, the headquarters moved from Windows 3.1 on some computers to Windows SP--in all a total of seven systems--each one requiring a little bit more in hardware. The same with the switching systems. It was a never-ending process.

(U) ~~(C)~~ Other important milestones included the recent establishment of the Chief Information Officer (CIO) and the ITMC (IT Management Council). Mitre and MICROSOFT consultants were also hired as resident experts. For example, if it had not been for these consultants, the establishment of the Portal would not have been possible. Another initiative has been the consolidation of databases within the headquarters. This was a key factor leading to the reorganization of the G-6/SI/CIO. Plans called for the Systems Integration (SI) to go awa, and its present resources that are involved in development will go to the G-3. Another highlight was the professional way in which headquarters G-6 types effected the transfer of all the information networks and telecommunications from the old to the new NGIC Building. It all went off without a hitch. And this was not the first time; the same efficient transfer took place when INSCOM elements moved from Fort Shafter in Hawaii to Fords Island. Recently, teams set up a new communications center at Pyong Taek in Korea. Over the

last 2 years telephone exchanges were replaced at the Nolan Building. However, there are problem areas. Traditionally, MSC's have operated independently because they were responding to and supporting different consumers. At the same time, it was essential that there be interoperability within INSCOM. (Presently, INSCOM possesses some 10,000 desktop computers.) Ideally, all hardware could be centrally purchased. Although this has not happened, there have been improvements. For instance, since 1999, the headquarters has centrally purchased software, and command-wide Information/Technology conferences are being held. This allows for increased dialogue. Finally, there is the area of visual information. Over the last several years, upgrades in VI have been neglected, largely due to the inability to effectively work the funding process. All the while the demand remains high for such support as video conferencing.

Foreign Language Technology Website. (U//~~FOUO~~) The need for translation of foreign languages in real-world operational environments has become critical and difficult to achieve with fewer linguistic assets. HQ INSCOM recognizes the need for more rapid foreign language technology "triage" applications in support of combatant commanders. A Foreign Language Technology web site was developed with seed money from HQ INSCOM, Office of the Assistant G3, Operations Readiness; the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (OASD C3I); and MITRE Corp. This effort provided the field with information available on government-off-the-shelf (GOTS) and commercial-off-the shelf (COTS) products and technologies for languages of interest to DOD.

501st Network Operations Center Consolidation. (U//~~FOUO~~) In October 1999, the 501st MI Brigade undertook the enormous task of consolidating subordinate battalion NOC operations and all associated communications assets into one building at the 527th MI Battalion. Project completion occurred in June 2000. This was followed by expanded NIPRNET LAN and SIPRNET LAN connectivity.

Headquarters Networks. (U//~~FOUO~~) HQ INSCOM operated four primary local and wide area networks providing connectivity to the NIPRENET (VULCAN), SIPRNET (FREY), JWICS (IDUN, and NSANET (THOR) backbone infrastructure. During the fiscal year, there was a continued effort to upgrade and expand

the server farm by obtaining 30 additional rack mounted servers. These servers were used to upgrade the email servers on all four local area networks (LAN), upgrade file and print servers, establish intranet/portal services on the SIPRNET and JWICS Lans. All Windows NT servers were migrated to Windows 2000 as the baseline. Also doing the year, efforts were underway to expand the SIPRNET LAN to meet the Command and Control requirements contained in the CIO's 5-year IT Plan.

(U//~~FOUO~~) The NIPRNET ATM backbone proved difficult to monitor and troubleshoot and did not provide the increased performance promised by the technology. So it was transitioned to GIGABIT, a process that went very smoothly and resulted in no interruption in service and in the end solved many real and perceived problems.

Information Dominance Center (IDC) Portal. (U/~~FOUO~~) In response to the terrorist attacks of 9/11, the CG INSCOM directed the creation of a worldwide portal as a follow-on to the making the IDC operational. The Chief Information Officer used Microsoft's Sharepoint Enterprise Portal Server to satisfy the tasking; this represented a new technology application for the command and accomplished command and intelligence community-wide collaboration and sharing of information. Because of classification issues, the JWICS network was the location of the portal which provided for higher classification because of its ability to limit user access. However, the G6 had to perform numerous upgrades to the backbone of the network and field a significant number of PCs to adequately meet the mission. As a measure of the portal's remarkable growth and wide dissemination, over one thousand users registered in a three week period.

Viruses. (U/~~FOUO~~) Three major viruses (NIMDA, Code Red, and SirCam) hit a variety of corporations and even some military organizations extremely hard during FY 2001. However, they were a non-issue at Headquarters, INSCOM. In addition, INSCOM was able to catch and clean tens of thousands of other viruses transmitted through e-mail.

(U/~~FOUO~~)

(b)(7)(E)

(b)(7)(E)

Mandatory Deployment of Systems Management Server (SMS). (U) The Automated Systems Integration Management (SIM) Intelligence Database (ASID) was INSCOM's primary tool for managing the IT investment through tracking and reporting the command's enterprise information infrastructure. Originally, ASID was a manual web-based process without the capability of automatic updates. In order to comply with the Chief of Staff, US Army guidance of 8 August 2001 and to make not only ASID but the IT management process more robust, INSCOM was forced to migrate to a more comprehensive solution and to add automatic discovery tools. The INSCOM Chief Information Officer then created a migration strategy for Microsoft's System Management System (SMS) and began fielding the system at several of the major subordinate commands. However, it was not all smooth sailing because of lack of full cooperation on the part of some of the subordinate commands.

CHAPTER FOUR

OPERATIONS

Unified Cryptologic System (USC) Transformation. (U//~~FOUO~~) The 1998 *Unified Cryptologic Architecture Study 2010,* commissioned by the Director of Central Intelligence and the Deputy Secretary of Defense, concluded that the Intelligence Community (IC), faced major technological and operational challenges, requiring a fundamental redesign of the SIGINT system. As Manager of the US Cryptologic System (USCS) and Community Functional Lead for SIGINT, the DIRNSA established the Unified Cryptologic Architecture Office (UCAO) to assist in the "fundamental redesign" of the IC through the implementation of a Unified Cryptologic Architecture (UCA). The UCAO developed an initial Master Transition Plan (MTP) by tailoring the Capability Maturity Profile (CMP) as outlined in DOD's study, *Architecture Framework,* dated October 2000. In short, the CMP evolved into the first MTP.

(U//~~FOUO~~) At the end of FY 2001, the various IC partners were drafting cost estimates for two options. These would then be evaluated by the Expanded Corporate Management Review Group. At the same time, Army intelligence was facing a "fundamental redesign" as a result of the Army Intelligence Transformation Campaign Plan and the Intelligence Electronic Warfare Modernization Plan. The challenge for Army leaders was to ensure synchronization with national and joint transformation efforts. Failure to do so could make Army cryptologic operations inconsistent within a transformed US Cryptologic System and could place the Army in danger of becoming non-interoperable and stove-piped and not contributing to the national SIGINT effort.

(S) (b)(1),(b)(3) Per CIA

(b)(1) (S) (b)(1)

(b)(1)

(b)(1)

(b)(1) (~~S//NF~~) (b)(1)

(b)(1)

(~~S//NF~~) (b)(1)

(b)(1)

(b)(1)

(b)(7)(E) (U//~~FOUO~~) (b)(7)(E)

(b)(7)(E)

(b)(1) (S//NF) (b)(1)

(b)(1)

(b)(1) (S//NF)

(b)(1)

(b)(1)

(S//NF) (b)(1)

(b)(1)

The Army's Relationship to the National Reconnaissance Office (NRO). (U) In an article that appeared in *Military Intelligence* magazine (April-June 2000), Colonel Donald L. Langridge outlined the background of the NRO and Army's relationship to it. What follows are excerpts from "Freedom's Sentinel in Space—the National Reconnaissance Office": (It should be noted no INSCOM spaces were involved in any of the internal Army elements mentioned as being connected with the NRO.)

(U) President Dwight D. Eisenhower secretly established a small, civilian-run office in the Pentagon in August 1960 to oversee a fledgling, experimental, military satellite reconnaissance program. Eisenhower thus set into motion a chain of events that, a year later, resulted in the founding of the organization known today as the National Reconnaissance Office (NRO), with responsibility for all US national-level overhead reconnaissance activities.

(U) Operating in near-total anonymity for the next four decades, the NRO succeeded in developing for the United States an unprecedented global capability to conduct sophisticated signals and photographic reconnaissance from space. This capability remains unmatched by that of any other nation to this day.

(U) As the United States' "eyes and ears" hundreds of miles overhead through the darkest days of the Cold War and beyond, NRO satellites have logged more than 40 years of distinguished service to the nation. As the country fights the War on Terrorism and faces new challenges in the 21st century, the NRO stands proudly as "freedom's sentinel in space.

(U) Publicly acknowledged for the first time in 1992, the NRO is a separate operating agency of the Department of Defense and one of the 13-member agencies of the national Intelligence Community. The

Secretary of Defense and the Director of Central Intelligence jointly manage the NRO. The NRO Director also serves as the Undersecretary of the Air Force.

(U) Since the Gulf War, the Army and the NRO have greatly strengthened their partnership. They are working hard to improve the support the NRO provides from space-borne reconnaissance assets to the combat forces planning for contingency operations, engaged in stability operations and support operations, and in actual combat. The Army now has three structures that work directly with and for the NRO. The Army Coordination Team (performs liaison functions), the Army Element (management of Army personnel assigned to NRO), and the Army Support Group (supported Army elements preparing for exercises and deployments) work in the areas of facilitating Army-NRO issues and internal NRO missions, and directly addressing Army Component requirements to meet the challenges of the future, respectively….

(S//NF)

(b)(1)

~~FOUO~~ ~~(S)~~ The Fall of the Wall occurred in 1990, with the subsequent demise of the Warsaw Pact and the USSR. The immediate effect of this event was a reduction in the frequency of SAEDA reports. The common perception of the USAREUR population was, "We won the war, and there is no intelligence threat anymore." The statistics from 1989 to 1998 remained very consistent. However, in 1998 there began a significant increase.

(b)(7)(E)

September 11 Legal Policy Changes. (U//~~FOUO~~) As a result of 9/11, there were greater changes in legal policy than in the law itself. For example, the Defense Authorization Act held only minimal change. Under the Patriot Act, law enforcement was granted greater flexibility in obtaining flasher warrants, but no new powers were specifically

created to help the Department of Defense. However, there was a temperature change that led to new policies. For example, it became easier under legal interpretation for counterintelligence and intelligence types to obtain for example credit histories. The important changes came as a result of sections 217 and 1003 of the Patriotic Act which created authority under the Electronics Privacy Act for a Third Party to monitor computer trespasses.

(b)(7)(E)

In the latter, it was possible to observe communications of those who hacked into Government communications. (In the past the ability to conduct this type of operations was based only on legal analogy.) For the first time, Congress came out and said that there was no expectation of privacy upon breaking into any public or private system. Prior to this, it had been the subject of an ongoing debate within DOD. At the same time, it should be remembered that this authority along with many of the other provisions of the Patriot Act are subject to a Sunset Provision wherein they will go away in December 2005 and the debate may be resurrected.

(U//~~FOUO~~) The Intelligence Act of 2002 witnessed the inclusion of the Coast Guard for the first time. This was significant because the Coast Guard was the closest thing the United States had to a *gendarmerie* such as in France or Belgium--a branch within the armed forces that possessed a law enforcement responsibility. For the most part, the Coast Guard comes under the Department of Transportation, but from time to time, they also fall under DOD. Congress acknowledged for the first time that the Coast Guard possessed an intelligence role that touched upon the protection of our borders and homeland security. For the first time, their intelligence role was being codified.

(U//~~FOUO~~) Looking to the future, many things that INSCOM wants to do are driven by policy not by statute and policy continues to evolve.

(b)(7)(E)

Finally, the various services have interests of their own in protecting their personnel. "Cyperspace is a unique place and we can't have agencies bumping up against each other." The bottom line is that law and doctrine will continue to evolve. There is also a

huge disconnect between the Foreign Intelligence Surveillance Act and the Electronics Communications Privacy Act. In the United States under domestic law, foreign agents have more protection than criminals. That is because the definition of "contents" under the Foreign Intelligence Surveillance Act prevents us from keeping such network data as telephone numbers or IP addresses. Whereas, the Supreme Court has granted law-enforcement this ability to record such information.

~~FOUO~~ ~~(S//NF)~~ (U) At this time, computer operations are probably the most important thing the SJA Office is involved in and requires constant legal scrutiny. Privacy is the watchword, and one simply can't do anything in this arena without legal guidance. When you decide to conduct an operation you require a legal review because the consequences are significant without one. To add to the normal challenges of 9/11,

(b)(7)(E)

Intelligence Oversight Issues. (U)

(b)(1)

INSCOM was the successor to the Army units involved. Consequently, the command took a very rigid stance in applying its oversight responsibilities, and lawyers began to become major players in operations. The INSCOM Intelligence Oversight Office itself promoted a very narrow, bureaucratic way of processing and reporting possible violations tempered with little judgment. In fact, it was becoming increasingly evident to those in human intelligence and counterintelligence that INSCOM was

adhering to a stricter interpretation of the law than anyone else in DOD, including other Army commands.

(b)(1)

For example, during DESERT STORM, INSCOM counterintelligence was initially paralyzed due to the absence of memorandums of understanding with the host countries while their counterparts in the other Services were going about traditional counterintelligence duties in support of arriving forces.

~~TOUO~~ (U) ~~(C)~~ Through the 1990's, with increased terrorism (and the lack of HUMINT/CI often taking the blame) and the coming of a new generation of leadership, changes slowly began coming within INSCOM.

(b)(7)(E)

As a departure from the past, the new director gave the local commander more flexibility in making the call.

(U) ~~(C)~~ September 11th only accelerated this change in culture, particularly as it related to the legal side and the involvement of lawyers. This did not mean that there were not continued struggles. For example, in Afghanistan there was a call as to whether or not they could video-tape prisoners. There was also a recent effort by the legal types to censure showing pictures of US target sites mentioned in documents found in Afghanistan.

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 42

IAGPA-CSF Form 6-R
1 Sep 93

(b)(1)

(b)(1)(b)(3) Per NSA (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Pre 9/11 Support to Counter Terrorism. (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)

(b)(1)

Army Counterintelligence Center. (U/~~FOUO~~) The Army Counterintelligence Center (ACIC) was the Army's only strategic counterintelligence analysis center. Located at Fort Meade, Maryland,

(b)(7)(E)

~~(C)~~ The Technology Protection Branch did most of the work. Its analysts possessed expertise in intelligence threats to specific technologies, weapons, and systems. For example,

(b)(1)

Finally, the Investigations and Operations Branch augmented counterespionage investigations by examining sensitive intelligence data for leads and by mining data sources previously unexploited.

(U) ~~(C)~~ The ACIC continued to use Intelink as the primary means for delivering finished intelligence studies to requestors. Over 90 percent of ACIC products were disseminated in soft copy, and studies were posted with 24 hours of release.

(b)(7)(E)

Since October 1997,

the ACIC had posted over 400 studies.

(b)(7)(E)

Prior to 9/11, the ACIC provided threat assessments for high-level travelers (senior Army and DOD officials). Assessments were also provided for site-specific locations as required. The Counterintelligence Periodic Summary summarized terrorist and CI events worldwide. Analysts inputted to command assessments that reported on threats to US Army interests worldwide.

NGIC's Reach to the Field. (U//~~FOUO~~) One way NGIC supported the commander on the ground was by enhancing the analytical capabilities of INSCOM's Theater Analysis and Control Elements. This was accomplished by using the concept of "reach," a virtual and collaborative process that allowed an ACE to access the center's knowledge base that included subject matter experts, intelligence products, and on-line databases. The end results were a more complete and detailed picture of enemy capabilities that the ACE could pass on to the Service Component Command, whose requirements were often greater than the Theater Joint Intelligence Center could provide.

(U//~~FOUO~~)

(b)(7)(E)

(U//~~FOUO~~) The NGIC used two types of organizations with which to support the ACE. The first was the NGIC Liaison Element, usually consisting of two personnel, who were assigned to the ACE in pre-deployment phase. They not only assisted the ACE in drawing the NGIC database but gained insights into the ASCC commander's requirements which facilitated the offering of "brilliant push" type of support. Secondly, the NGIC Crisis Action Team (CAT) were

activated at the onset of a crisis or exercise and were able to undertake 24 hours-a-day operations. (The team also grew upon other organizations such as the Army Counterintelligence Center (902d MI Group) for expertise.) The CAT monitored the friendly and opposing force situation, managed Requests for Information, directed "smart pulls" or "brilliant pushes," and facilitated collaboration and coordination with other headquarters. Finally, NGIC's Imagery Crisis Response Cell and the Army Imagery Requirements Office were also capable of operating on a round-the-clock basis to support crises or exercises.

~~(S//NF)~~

(b)(1)

~~(S//NF)~~

(b)(1)

(b)(1)

(U) ~~(S//NF)~~ During the year, significant problems arose regarding soldier deployments in support of sensitive non-Army, DOD activities. In some instances Secretary of the Army and CG, INSCOM prerogatives were being ignored by the supported organizations, resulting in unnecessary risks to soldiers and the entire ACP. As a result, clarifying guidance was issued that resulted in improved efficiency of support and reduced soldier and mission risk.

(b)(1) **Activities.** ~~(S//NF)~~ Besides its HQ INSCOM element, maintained a collection management element within NSA (b)(1)(b)(3) Per NSA for the purpose of coordinating information requests and subsequently tasked (b)(1) units worldwide. (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

~~(TS~~) During FY 2001, NSA presented (b)(1) Detachment (b)(1)(b)(3) Per NSA with the National Intelligence Meritorious Unit Citation. The basis of the award was (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

The operation was a joint effort between the Defense HUMINT Service and (b)(1) (b)(1)(b)(3) Per NSA

Polygraph Program. (U//~~FOUO~~) INSCOM's Polygraph Program conducted 1,792 CSP examinations. Of these 1,737 were no significant responses; 40 were inconclusive; 15 were significant responses; and 11 were no opinion. The command had a 94.8 percent overall resolution rate; a 2 percent non-support rate; and a 13 percent admission/deception indicated confirmed. The program completed 67 operational cases of which 58 were no deception indicated; 4 were inconclusive; 4 were deception indicated; and 1 tested no

opinion. Following the DOD Polygraph Institute Quality Assurance Program's inspection, it lauded the INSCOM polygraph program as one of the best.

(U/~~FOUO~~) Two INSCOM polygraph examiners (from the 66th and the 902d MI Groups) conducted 32 security screening examinations in Sarajevo and Tuzla, Bosnia-Herzegovina. This involved screening of civilian local hires for Stabilization Forces (SFOR). An evaluation of the process was to be used in determining the feasibility of making such screen test a routine part of SFOR's force protection program.

(b)(1) (b)(1)

(b)(1)

Deployable systems supported throughout FY 01 included several deployments of (b)(1) in exercise and contingency scenarios; rotational redeployments of the three STEAMROLLER (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA for refurbishment without a drop in effective coverage (INSCOM received 1.3 million dollars from DA/NSA) to retrofit and increase communications bandwith); numerous contingency and exercise deployments of all echelon (b)(1) and following 9/11, facilitated uninterrupted and assured high data rate secure communications for the WMD CST UCS. (On 9/11, 10 additional vans were fielded.)

EAC Information Operations Requirements. (U//~~FOUO~~) An internal plan looked at INSCOM's IO requirements for the near-term. In the plan, increased anti-terrorism counterintelligence support (including personnel) as mandated by the Cole Commission's findings and endorsed by the Chief of Staff, US Army were addressed. Under the

plan, a robust all-source analytical cell would be created that would provide "reach" support to the overall force protection mission. The plan also addressed the need for "information superiority" and called for the consolidation of all IO functions at INSCOM. But for all of this to happen, was a need for more resources.

501st (b)(1) ~~(S//NF)~~ During the year, the 501st MI Brigade operated four (b)(1) (b)(1) These included a focus on growing threats from (b)(1) (b)(1) (b)(1) (b)(1) the 501st that would address early warning and force protection reporting of terrorist acts.

~~(S//NF)~~

(b)(1)

~~(S//NF)~~

(b)(1)

Combat Development Target. ~~(TS/~~ (b)(1) The G3 alerted the Intelligence Community (b)(1) (b)(1)

General officers from STRATCOM were briefed on the matter leading to requests for additional information. The G3 also briefed Taiwanese officials (b)(1)

(b)(1)

Deployment of the G3 Information Operations Warfare Activity (IOWA) Team. ~~(S//NF)~~ The USFK and EUSA established an operational need for the development of exploitation and electronic warfare systems to counter a North Korean (b)(1)

(b)(1)

Smugglers. ~~(S//REL UK)~~ C Company, 66th MI Group passed actionable (b)(1) information to Task Force Falcon that led to the detention of two possible smugglers and the seizure of military uniforms and flak vests in the vicinity of Lovce, Kosovo, on 29 March. Three days later, the Army Europe (b)(1) provided tip-offs that allowed for the arrest of two more suspects near Podgrade, Kosovo. These

(b)(1)

~~(S//NF)~~

(b)(1)

USN EP-3 Crisis. ~~(TS~~) In April 2001, a disabled USN EP-3 reconnaissance plane collided with a PLAAF fighter and

was forced to land in China. Linguists (b)(1)(b)(3) Per NSA Group shouldered the majority of the workload (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA providing critical insights to the National Command Authority that passed the information on to Ambassador Prueher at the bargaining table. Up to the release of the crew, (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

MRSOC Role. (~~S~~) The Medina Regional Security Operations Center first (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Significant IIR. (C/~~NF~~) The Kaiserslautern MI Detachment, 66th MI Group, published a FORMICA interim intelligence report (IIR) (b)(1) (b)(7)(E)

(b)(7)(E)

CI Support to Force Protection. (C//~~NF~~) The 205th MI Battalion, 500th MI Group sent a three-person CI team (b)(1) (b)(1) to provide force protection for a USARPAC engineer platoon that was building a hospital annex (b)(1) as part of the CINC's Theater Engagement Plan. The CG USARPAC ordered the activation of the CI team in response to increased activity of a Maoist insurgency group and a rising civil unrest (b)(1) The CI team conducted vulnerability assessments, limited analysis, and liaison support (b)(1)

(b)(1)

(b)(1)

(b)(1) This was significant in that for the first time this computer-to-computer capability would take computer network attack beyond hacking/cracking into network operations that supported the operations.

(b)(1)(b)(3) Per NSA ~~TS~~, (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

~~TS~~,

(b)(1)

(S//NF)

(b)(1)

International Crime. (S/) SIGINT specialists from the 704th worked at NSA's International Organized Crime Branch

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA (S/) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(S//NF)

(b)(1)

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1); (b)(1) & (b)(3) per NSA

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 54

66th Intelligence Information Report. ~~(C//NF)~~ (b)(1)

(b)(1)

Support to Counter-terrorism. ~~(S//NF)~~

(b)(1)

Counterdrug. (~~TS~~, ~~NF~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

New SIGAD. (~~U~~) On 3 August 2001, the National Security Agency assigned the SIGINT Activity Designator (SIGAD) (b)(1)(b)(3) Per NSA to the INSCOM Information Dominance Center (IDC). This allowed the IDC to conduct SIGINT within the NSA/CSS charter. (The goal of IDC was to provide Army-wide real-time indications and warnings of counter-terrorism, counterintelligence, information operations, counternarcotics, and force protection.) (b)(1)(b)(3) Per NSA comprised the SIGINT development and analytic effort associated with the CG INSCOM's initiative of enhancing counter-terrorism indications and warnings support for force protection. As the FY 2001 came to an end (b)(1)(b)(3) Per NSA was still a work very much in process.

(b)(1)(b)(3) Per NSA

Threat Assessments. ~~(S//NF)~~ (b)(1)

(b)(1)

(b)(1)

(b)(1)(b)(3) Per NSA **Support to Task Force Eagle (TFE).** (~~S~~) (b)(1)(b)(3) Per NSA continued to provide Indications and Warning and Force Protection support to TFE. In one instance, the AETCAE (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Waiver to Collect. (~~S~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Uninhabited Aerial Vehicle. (U/~~FOUO~~) In an article "March of the Robots," John D. Gresham wrote on the background of the uninhabited aerial vehicle (UAV).

(b)(7)(E)

Current systems being tested included the prototype helicopter UCAV armed

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

with Hellfire ASM on an old QH-50 DASH drone. Army engineering and ordnance disposal units had also made use of robots for years to support vital and dangerous tasks. In late October 2001, the entire DOD UAV program achieved a milestone when an RQ-1 was used in Afghanistan (Operation ENDURING FREEDOM) to target and then fire an AGM-114 Hellfire air-to-surface missile (20 lb warhead) guided by a laser.

(U//~~FOUO~~) The big question that remained unanswered was the role UAV would play in the Army's Future Combat System, currently a "paper" system designed to replace heavy Cold War-era fighting vehicles like the M1 Abrams and M2/3 Bradley. (b)(7)(E) Looking to the "possible," the UAV could serve as an off board sensor/weapons platform.

115th Support to ENDURING FREEDOM. (~~TS~~) The group's most visible contribution to the campaign was to the tactical customers prosecuting the war. The Warfighter SIGINT Integration Cell, along with the USARPAC RTCAE, provided a (b)(1)(b)(3) Per NSA to CENTCOM collection managers. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA Support also existed in the form of real-time threat warning. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

9/11 Changes to IDC Capabilities. (~~S~~) (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

Uniqueness of the IDC. (~~TS~~) The Information Dominance Cell searched for the electronic network developed when communication occurred, and for the intelligence inherent in these relationships for cross-cueing the other intelligence disciplines. The IDC was a congregation of powerful search and analytical tools (COTS/GOTS), simultaneously coupled to available databases (IMINT, HUMINT, and SIGINT), (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

INSCOM Support to the Tactical Commander. (U//~~FOUO~~) Within each unified command, INSCOM intelligence support served as the primary conduit for intelligence information between the tactical command and national and other military services' intelligence organizations. Additionally, the Army tailored the theater intelligence brigades and groups specifically to the meet the requirements of the various Army Service Component Command (ASCC) commanders and to support the various unified commanders. An important part of INSCOM's larger effort was to provide intelligence support to the lowest possible tactical echelon, and when S2s effectively leverage INSCOM capabilities, they were able to significantly increase the intelligence support they could provide to their commanders. The primary means of exploiting this capability was through the use of effective requirements management (RM) or mission management (MM). Although a maneuver brigade or battalion could not directly task an EAC intelligence support element, it could leverage the capabilities through the RFI

process. However, one common problem with RFIs was that the request was too vague to answer.

Future Challenges. (U) As part of the Association of US Army's Intelligence Symposium held at DIA in August 2001, LTG Robert W. Noonan, Jr., DCSINT outlined a number of trends impacting upon the Army and its intelligence arm in the future. The first was that unlike the past, future conflicts will be fought in urban terrain. By 2020, 66 percent of the world's population will live in these urban areas. Secondly, the Army must maintain its technology edge in weapons and intelligence systems. This meant that Army intelligence must get its arms around technology transfer so that the Army can be prepared. Finally, the proliferation of information was making the world one global village.

CERT Support. ~~(TOUO)~~ The ACERT (Army Computer Emergency Response Team/Coordination Center) and the RCERTs (Regional CERT) responded to 14,641 incidents on Army computer systems/networks in FY 01, which was again, as in FY 00, a dramatic increase in the number of recorded incidents compared to the previous year. The breakdown was 31 denial-of-service attempts, 98 intrusions, 12,744 probes/scans, 1201 access attempts, 219 poor-security practices, 298 malicious logic incidents and 50 incidents of unknown origin.

ADDENDUM

(The INSCOM History Office was made aware of the following information too late to be included in earlier summaries.)

(b)(1) **DHS.** ~~(S,~~) In June 1993, the Department of Defense offered up a study that would create a Defense HUMINT Service (DHS). Under this proposal, all of General Defense Intelligence Program resources of DIA and the military services would be consolidated into a single agency under DIA's control.

(b)(1)

~~(S.~~)

(b)(1)

Regraded SECRET on 16 Jan 2014 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R

~~(S.~~) As a compromise, (b)(1) created a memorandum of understanding that align the program with the new Defense HUMINT Service while at the same time, maintaining its independence. For instance, (b)(1) would place representatives at various DHS operational bases (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA Mr. (b)(6) and (b)(1) would also maintain an office at DHS. (This was later eliminated when NSA sent its own person to DHS to represent all SIGINT

interests.) All these actions ensured synergy between (b)(1) and the larger Defense HUMINT effort.

Chief Information Officer. (U) The Chief Information Officer began as a concept borrowed from industry and applied by Congress in the 1996 Clinger-Cohen Act to help redesign government and dramatically change the way business was conducted. In 1996, DOD named the ASD/C3I as its CIO and the Services and Agencies rapidly followed suit. (The Director of Information Systems Command, Control, Communications and Computers (DISC4) was appointed as the Army's CIO.) In January 2000, INSCOM created its CIO on the basis of AR 25-1. The mission was to procure, build, manage, and maintain an achievable, collaborative, worldwide Army Intelligence enterprise solution that linked INSCOM with its units, partners, supported and supporting agencies, and managed future information management and information technology (IM/IT) investments. The CIO represented a new way of doing business and had the authority to look across the entire command regarding IM/IT issues.

FY 01 UNIT SUMMARIES

National Ground Intelligence Center

History: (U) With the breakup of the Army Intelligence Agency, two of its principal parts (the USA Foreign Science and Technology Center (FSTC) and the USA Threat and Analysis Center (ITAC)) were reassigned to INSCOM on 10 April 1992. On 1 October 1995, these two separate entities went away and their functions were merged into the newly created INSCOM National Ground Intelligence Center.

Location: (U/~~FOUO~~) From its creation, NGIC was located in Charlottesville, Virginia. However, on 21 September 2001, the center dedicated the Nicholson Building on 2055 Boulders Road as its new permanent home. (For more about the building see the write-up on the "Nicholson Building" elsewhere in this history.)

Mission: (U/~~FOUO~~) The NGIC produced and disseminated all-source integrated intelligence on foreign ground forces and supporting combat technologies to ensure that US forces had a decisive edge on any battlefield. The NGIC represented a true synthesis of general Military Intelligence (GMI) and scientific and technical intelligence (S&TI)—a one-stop shopping.

Organization: (U/~~FOUO~~) Internally, NGIC consisted of four major elements: The **Forces Directorate** was made up of area and military specialists studying current and future foreign ground forces from the operational level down to the small unit level. These studies were used to help plan scenarios, analyze costs of proposed defense programs, furnish information on foreign adversaries to the Center of Army Analysis, and provide information to the USA Training and Doctrine Command for use in building force structures. Within the **Ground Systems Directorate**, scientists and engineers utilized a variety of unique capabilities (such as the ELINT laboratory, Compton Compact Radar Range, Joint Assessment of Catastrophic Events Model, the Geographical Information Systems, and the Digital Imagery Operations Center, etc.) to evaluate any type of equipment or weapons that might threaten the US Army. The NGIC's Foreign Materiel Program focused on acquiring and exploiting foreign ground systems and helicopters. And finally, there was the **Imagery Assessments Directorate** located at the Washington Navy Yard in the District of Columbia. The directorate produced a wide-range

of imagery intelligence products and served as NGIC's most direct link to the war-fighter. A special strength of the imagery effort was its imagery-based modeling tools, such as the Integrated Assessment of Chemical Production Facilities. On 15 June 2001, the **203d MI Battalion**, which supported NGIC's technical intelligence mission, was inactivated at the Aberdeen Proving Ground, Maryland. In its place was created a Multi-Compo unit using personnel drawn from INSCOM and the Reserves. (See write-up on "Coming of Multi-Compo Units.")

Operational Highlights: ~~(S//NF)~~ Prior to 9/11, imagery support was being provided to warfighters deployed in Kosovo, Bosnia and Kuwait.

(b)(1)

Regraded SECRET on
16 Jan 2014
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

513th MI Brigade

History: (U) The 513th was stood up in 1982 to support the ground component of the US Central Command during contingencies in Southwest Asia. Over the years, the 513th MI Brigade became INSCOM's power projection brigade with potential worldwide focus.

Location: (U) In 1994, the 513th MI Brigade was relocated from Fort Monmouth, New Jersey, to Fort Gordon, Georgia, where it remains along with its 201st, 202d, and 297th MI Battalions. However, the 204th MI Battalion is currently located at Fort Bliss, Texas.

Mission: (U/~~FOUO~~) The 513th MI Brigade conducted theater level multi-discipline intelligence, force protection, counter-drug, electronic warfare, and information operations in support of US Army South, US Army Central Command, and other deploying forces.

Organization: ~~(C)~~ The 513th mission is divided among four battalions: The **201st MI Battalion** at Fort Gordon which was responsible for SIGINT in support of theater army components, and MASINT in support of national requirements. A Company performed SIGINT collection and direction finding and D Company conducted MASINT and manned a Technical Control and Analysis Element (TCAE). (Besides manning the Technical Control and Analysis Elements at Fort Gordon, soldiers of the 201st MI Battalion operated the TCAE (b)(1)(b)(3) Per NSA D and E Detachments and F Company were attached to (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA where they performed similar responsibilities.

~~FOUO~~ ~~(C)~~ (U) The **202d MI Battalion**, also at Fort Gordon, provided counterintelligence and human intelligence in support of theater army components.

(b)(7)(E)

(During FY 2001, the 202d had a company forward in support of the US Army South in Puerto Rico and also maintained a forward presence in Kuwait (Field Office Southwest Asia), Qatar, and Saudi Arabia).)

~~FOUO~~

~~(C)~~ The **204th MI Battalion** served as the Army's only echelon above corps aerial battalion and consisted of highly

sophisticated, multi-sensor aircraft and tactical ground downlink equipment and teams capable of deploying worldwide independently or as part of the 513th. (Presently, the battalion's main effort was directed in support of the counter-drug war efforts of the US Southern Command.)

(b)(7)(E)

~~FOUO~~ (U) ~~(C)~~ Finally, the **297th** at Fort Gordon served as the operations battalion for the 513th MI Brigade.

(b)(7)(E)

(In December 2001, these systems were scheduled to be replaced by the Tactical Exploitation System (TES)). The 297th also supported manning of Intelligence Support Elements at Fort Bragg, North Carolina; Fort Hood, Texas; Fort McPherson, Georgia; Camp Doha, Kuwait; and Eskan Village, Saudi Arabia.

~~(S)~~

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 66

IAGPA-CSF Form 6-R
1 Sep 93

66th MI Group (Provisional)

HISTORY: (U) The 66th MI Group (Provisional) was established on 16 October 1997 upon the inactivation of the 66th MI Brigade.

LOCATION: (U/~~FOUO~~) In June 1998, the 66th relocated from Augsburg, Germany, to the Dagger Complex and Kelley Barracks in Darmstadt. Besides the Dagger Complex, operations were conducted from Bad Aibling, Stuttgart, Heidelberg, etc. All together, the 66th had elements in six European countries and forward deployed personnel in Kosovo and Macedonia.

MISSION: (U/~~FOUO~~) USAREUR's intelligence requirements covered a wide and complex spectrum of possible missions and operations in or out of the USEUCOM Area of Responsibility that included more than 89 countries and encompassed the entire spectrum of military operations. (b)(7)(E) The 66th was required to provide direct support to USAREUR, Southern Europe Task Force (SETAF) and 21st Theater Support Command (TSC), and to provide reinforcing support to V Corps along with other units within the USAEUR/EUCOM AOR. The 66th also responded to USAINSCOM, national level tasking authorities, and/or service agreements.

ORGANIZATION (C) (~~U/FOUO~~) Internally, the 66th MI Group was divided between the **Directorate of Operations** (responsible for (b)(1) (b)(1) and the **Directorate of Investigations** (oversaw all counterintelligence and human intelligence activities). The 66th MI Group began FY2001 consisting of a Headquarters company, C Company, and an Operations Battalion. It was also assigned (b)(1) (b)(1) C Company and Operations Battalion went away on 16 January 2001 when the **533d MI Battalion (Prov)** was organized in their place. The 533d was further broken down into a Headquarters Company, A Company (Operations), Bravo Company (CI/interrogations), and C Company (b)(1) C Company was located at Bad Aibling in concert with the 108th MI Group/field station. In addition, in theater elements of the 513th were

attached to 66th and performed (b)(1) responsibilities.

OPERATIONAL HIGHLIGHTS: (U/~~FOUO~~) Daily duties of the 66th included preparation of a briefing for intelligence officers at USAREUR and KFOR J2. If required, the 66th provided a large-picture intelligence focus for operational elements through use of its Deployable Intelligence Communications System, a reach-back capability to exploit the data gathered for the European Command, National Authorities, and other operational forces. The 66th also determined threat assessments and provided force protection through the exploitation of human resources. During FY 2001, the 66th assisted in the research of information for personal security clearances.

(b)(7)(E)

108th MI Group

HISTORY: (U) The 108th MI Group was activated on 16 June 2000 to replace the TDA organization, 718th MI Group. During FY 2001, the 108th undertook planning for an uncertain future. See write up elsewhere on closeout.

LOCATION: (U/~~FOUO~~) Bad Aibling Station was located in the town of Mietraching, just outside Bad Aibling, Germany. Its headquarters was located in Building 301. The Operations Compound was housed in Buildings 325, 325A, and 340.

MISSION: ~~(U/~~(b)(1) The 108th had (b)(1) communications security responsibilities. Its primary mission was to (b)(1) (b)(1) that supported the National Command Authority, strategic consumers, and tactical warfighters. The types of operations being supported included combat, peace-keeping/enforcement, humanitarian/disaster relief, non-combat evacuation, show-of-force, search and rescue, and counter-terrorism.

ORGANIZATION: ~~(TS~~(b)(1) The 108th MI Group was divided into four directorates to include the **Directorate of Operations** which was further divided into the (b)(1) (b)(1) (b)(1) the Support Activity provided value added (b)(1) to deployed US forces. (b)(1) (b)(1) (b)(1) Finally, the 108th MI Group commanded the 401st MI Company.

OPERATIONAL HIGHLIGHTS: ~~(TS/~~(b)(1) (b)(1)

109th MI Group

HISTORY: (U) On 16 June 2000, the 109th MI Group was activated to replace the discontinued 713th MI Group, a TDA counterpart.

LOCATION: (U/~~FOUO~~) Menwith Hill Station is located near Harrogate, England. Elements of the group were also located at Molesworth and Digby.

ORGANIZATION: (U/~~FOUO~~) The 109th MI Group over saw a Headquarters Detachment, the Molesworth Element, the Digby Element, and the 404th MI Company.

OPERATIONAL HIGHLIGHTS: (~~TS~~/(b)(1)) Menwith Hill continued to provide timely intelligence to force protection efforts in support of Operations NORTHERN WATCH and SOUTHERN WATCH and in Kosovo. The Menwith Hill Station (b)(1)

(b)(1)

902d MI Group

HISTORY: (U) The 902d MI Group had been assigned to INSCOM since 1977. However, through the years it underwent a series of reorganizations that left it in sole control of INSCOM's counterintelligence mission. In 1996, the Foreign Counterintelligence Activity was assigned, and the 308th and 310th MI Battalions activated as replacements for TDA counterparts.

LOCATION: (U/~~FOUO~~) The 902d MI Group Headquarters and subordinate Battalion/Activity Headquarters were all located at Fort George G. Meade, Maryland. In addition, the 902d MI Group had Company Headquarters, Detachments, and Resident and Field Offices in 27 other CONUS/OCONUS locations.

MISSION: (U/~~FOUO~~) The 902d MI Group conducted multidiscipline counterintelligence operations throughout CONUS and designated worldwide locations to detect, neutralize, defeat, and exploit the threat to US Army forces, secrets, and technologies, with emphasis on countering Foreign Intelligence Services. During contingencies, the 902d MI Group reinforced designated units with tactically tailored CI deployment packages or individual augmentation in support of Theater Commanders during peacetime, Security and Stability Operations, and major regional conflicts.

ORGANIZATION: (C)

(b)(1)

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

☒ Information has been withheld in its entirety in accordance with the following exemption(s):

(b)(1)

It is not reasonable to segregate meaningful portions of the record for release.

☐ Information pertains solely to another individual with no reference to you and/or the subject of your request.

☐ Information originated with another government agency. It has been referred to them for review and direct response to you.

☐ Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

☐ Other:

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 72-73

704th MI Brigade

HISTORY: (U) The brigade's origins can be traced back to 1954 and the move of the National Security Agency from Arlington Hall Station, Virginia, to Fort George G. Meade, Maryland. Through the years, the brigade continued to command personnel and units whose missions were to support NSA.

LOCATION: (U) ~~(S)~~ The 704th MI Brigade, its Headquarters Company, and the 741st and 742d MI Battalions were all located at Fort Meade, Maryland. (The Command Group of the 704th was located in Building 9805; the 741st was in 9828; and the 742d Battalion in 9802.) However, the 742d had a detachment in Utah working alongside the 300th MI Brigade (Utah National Guard); the 743d MI Battalion was headquartered in Building 1219, Fort Carson, Colorado, but also had detachments at various CONUS and OCONUS sites (including Winter Harbor, Diego Garcia, and CSGAS).

MISSION: ~~(TS//SI//TK)~~ The Brigade supported warfighters and national decision-makers' information superiority requirements through the conduct of Signals Intelligence, Information Security, and Information Operations both directly and through support to the National Security Agency. The mission of the **741st** was to conduct SIGINT operations (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA as well as provided support to NSA's various operational groups. The **742d** was to conduct operations in support of Army requirements, in support of NSA operations, provide technical SIGINT support to FORSCOM, and to exercise operational control of the 300th MI Brigade (National Guard). Finally, the focus of the **743d** was on worldwide SIGINT missions in support of strategic commanders and indirectly to operational and tactical commanders and facilitated the planning and execution of the Army Space Command.

ORGANIZATION (U) ~~(C)~~ The Brigade's Headquarters Company included senior Army personnel assigned to joint duty positions within the US Army Element of the National Security Agency. (The US Army Element remained a separate TDA organization on paper only.) Personnel assigned to the 741st MI Battalion were almost all employed within the Operations Directorate, NSA. The 742d MI Battalion operated the Army Technical Control and Analysis Element furnished soldiers to NSA support groups. The finally, the 743d MI Battalion as indicated above supported strategic commanders.

OPERATIONAL HIGHLIGHTS: (~~TS~~) A 704th soldier assigned to the Office of International Organized Crime Branch led a team

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA Members of the 704th also participated in an important brief (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA The discussions centered

(b)(1)(b)(3) Per NSA

116th MI Group

HISTORY: (U) On 16 June 2000, the 116th MI Group was activated replacing the 702d MI Group as part of a command-wide effort to present a TOE face.

LOCATION: (U/~~FOUO~~) The 116th Group remained located at Fort Gordon, Georgia, where it oversaw the Gordon Regional Security Operations Center. The 206th MI Battalion was collocated with its parent unit at Fort Gordon. In direct support to the Medina Regional Security Operations Center (MRSOC), the 314th MI Battalion was located at Lackland Air Force Base, San Antonio, Texas.

MISSION: (U/~~FOUO~~) As host unit, the 116th MI Group provided personnel and support to the Gordon RSOC and integrates Reserve Component soldiers into the center's operations. The 314th MI Battalion served as the Army component of the Medina RSOC where the battalion provided SIGINT information to satisfy warfighting and national level intelligence requirements.

ORGANIZATION: (U/~~FOUO~~) The 116th MI Group controlled the 206th MI Battalion and the 314th MI Battalion. The **206th Battalion** was broken down into a Headquarters and Headquarters Company, A Company, and E Detachment. (b)(7)(E) The **314th MI Battalion** had three companies and a detachment: Headquarters and Headquarters Company, A Company, B Company, and D Detachment. Mirroring its sister battalion, the 314th MI Battalion's A and B Companies consisted of linguists and analysts assigned to the MROC, and D Detachment served as the Medina RTCAE.

OPERATIONAL HIGHLIGHTS: (S) The 314th MI Battalion expended much of its energy preparing for (b)(1)(b)(3) Per NSA transfer from (b)(1)(b)(3) Per NSA to the MRSOC. An Integrated Military Operations Division within the J31 to coordinate the transfer. Following 9/11, the GRSOC and MRSOC, in coordination with NSA's Office of Regional Targets, were given new target responsibilities. (b)(1)(b)(3) Per NSA (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA As a force provider to both the GRSOC and MRSOC, the 116th MI Group remained the center of gravity of NSA/CSS support to CENTCOM and EUCOM for the Middle East. As the host for GRSOC, the 116th was given the added task of re-configuring the GRSOC's infrastructure and support systems.

115th MI Group

HISTORY: (U) The 115th MI Group was activated on 16 June 2000 to replace the 703d MI Brigade as part of a larger effort of INSCOM to offer a TOE face.

LOCATION: (U/~~FOUO~~) The 115th MI Group occupied two principal locations on the island of Oahu, Hawaii. Operations were conducted at the Kunia Tunnel, bordering Schofield Barracks. The group's headquarters was in Building 130 on Schofield Barracks, and its subordinate battalion headquarters was in Building 131.

MISSION (U) ~~(C)~~ The 115th Military Intelligence Group, as the Army component of the jointly staffed Kunia Regional Security Operations Center (KRSOC), conducted joint signals intelligence operations responsive to warfighter and national requirements and deployed individuals to reinforce forward-based units. The group provided approximately one-third of the KRSOC Operations Directorate operations, management, training, and plans staffs. Additionally, the 115th provided administrative support to soldiers assigned to the 205th MI Battalion (500th MI Group) who operated the Regional Technical Control and Analysis Element at Kunia.

ORGANIZATION: (U/~~FOUO~~) Besides its Headquarters and Headquarters, Detachment, the 115th MI Group controlled the **406th, 407th, 408th,** and **409th MI Companies.** (To oversee these companies, the group created a provisional battalion (**732d MI Battalion**) using personnel from its Headquarters Detachment.)

OPERATIONAL HIGHLIGHTS: (~~TS~~) (b)(1)(b)(3) Per NSA

(b)(1)(b)(3) Per NSA

USAINSCOM Land Information Warfare Activity

HISTORY: (U/~~FOUO~~) LIWA's roots dates back to 1995 when an element was established at HQ INSCOM to participate in the information operations/warfare arena.

(b)(7)(E)

LOCATION: ~~(FOUO)~~

(b)(7)(E)

However, key support elements are scattered throughout CONUS and are in Korea, Germany, and Hawaii.

MISSION: ~~(FOUO)~~

(b)(7)(E)

coordinates and synchronizes support from INSCOM, Army, and other Services, the Joint IO community, and other Government activities. It projects capabilities around the world to provide offensive and defensive IO operational, planning, and training support to land component commanders.

ORGANIZATION: (~~TS~~) The Information Dominance Center was a congregation of powerful search and analytical tools,

(b)(1)

(b)(1)(b)(3) Per NSA

On 3 August 01, the National Security Agency assigned the SIGINT Designator [redacted] to the IDC. (This was a part of General Alexander's vision of offering "one-stop intelligence and information operations shopping.") The change in operations also led to organizational changes. Although no formal permanent orders were published, on paper, the IDC was established as a separate entity under the CG, INSCOM, and the commander of LIWA also wore the hat of Commander, IDC. Underneath of the IDC were the Intelligence Operations Center (from the G-3, HQ INSCOM), the LIWA, Futures Center, and Cyber

Warfare Center (CWC). The LIWA itself was divided between a Director of Support and a Director of Operations.

OPERATIONAL HIGHLIGHTS: ~~(FOUO)~~ At the end of the year, LIWA had an authorized/actual strength as follows: officers 62/37, warrant officers 10-16, enlisted 53/47, and DA civilians 85/76 for a total of 210/176. Based on its FY 04-09 Program Objective Memorandum (POM) submission, LIWA submitted requirements for 70 officers, 25 warrant officers, 115 enlisted, 167 civilian, and 234 contractor-equivalents.

~~(FOUO)~~

(b)(7)(E)

Complete graphical topology diagrams were supplied by node, base camp, and layer 2/3 device. This was the first such product produced for the SFOR and was viewed as invaluable to improving the overall security and administration of the theater networks.

~~(FOUO)~~ Do-It-Yourself Vulnerability Assessment Program (DITYVAP) became a major thrust for the year. Training personnel to carry out this mission was an ongoing mission. This included training Regional Computer Emergency Response Team (RCERT) personnel to conduct the training and training Active, Reserve, and National Guard personnel. At the close of FY 01, 187 personnel had completed mandatory Information Systems Security Monitoring (ISSM) training: 198 have completed level-1 scanning training; 45 have completed analysis level-2 training; and 9 completed level-3 supervisory training.

500th MI Group

History: (U) The 500th MI Group has been in existence, except for one brief period, from 1952, and thus has earned the title of the "Pacific Vanguard."

Location: (U) The headquarters of the 500th MI Group continued to be located at Camp Zama, Japan, with major subordinate detachments at Misawa Air Base, Yokota Air Base, Kure, Tokyo, and Yokohama, and Okinawa, Japan; Fort Shafter, Hawaii; Republic of Marshall Islands; Alaska; and Fort Lewis, Washington. (Many of these were forward-deployed CI detachments.)

Mission: (U) The 500th MI Group provided intelligence support to US Army, Pacific and engaged Asia-Pacific intelligence and security institutions in order to contribute to regional stability and crisis response. As directed, provided support to joint and national agencies.

Organization: ~~(C)~~ The 500th MI Group oversaw (b)(1) (b)(1) the 403d MI Detachment (b)(1) and the 205th MI Battalion (b)(1) In addition, there were three smaller elements: The Security Liaison Detachment, the COMTECH Detachment, and the Counter Intelligence Detachment Japan.

Operational Highlights. ~~(S/NF)~~ In March 2001, the 205th deployed a small CI team (b)(1) to provide intelligence support to force protection for an engineer platoon building a hospital. (b)(1)

(b)(1)

501st MI Brigade

History: (U) Its entire existence has been in providing intelligence and security support to US forces in Korea: First, as part of the Army Security Agency during the Korean War. Secondly, since being activated in 1978, the 501st became a part of the newly created US Army Intelligence and Security Command.

Location: ~~(POUO)~~ The 501st MI Brigade along with a number of its elements were located at Sobingo Compound, outside of the US Yongsan Military Reservation, Seoul, Republic of Korea. The same for the 532d MI Battalion. The 3d MI Battalion was at Camp Humphreys, Pyongtaek; the 524th MI Battalion at Zoeckler Station, Camp Humphreys; and the 517th MI Battalion also at Zoeckler Station.

Mission:

Organization: The 501st MI Brigade

Operational Highlights: